

LA LETTRE D'INFORMATION

N°12 Direction de la Sécurité Économique en Zone Paris

EDITO

Alors que le trimestre semble à peine avoir débuté, voilà que se profilent déjà les fêtes de Noël. Loin de moi l'idée de vouloir dresser un bilan de l'année écoulée mais permettez-moi de partager avec vous quelques unes des tendances que nous avons pu discerner jour après jour. Elles seront développées dans cette nouvelle lettre d'information.

En tout premier lieu, l'accent est mis sur le cyberespace, terme polymorphe qui mérite, à mon sens, un éclaircissement pour mieux permettre d'en cerner les enjeux.

Ensuite, le besoin d'une information pertinente est devenu crucial, tant pour les entreprises que les institutions. C'est pourquoi, la DSEZP a mis en place une journée de formation complémentaire des OS. Se voulant pragmatique, elle a permis à 30 d'entre vous d'approfondir leurs connaissances en matière de protection, de réglementation, etc. La première édition a atteint ses objectifs et l'expérience sera donc pérennisée en 2017.

Ces diverses initiatives sont autant de jalons qui manifestent notre volonté d'être à vos côtés pour protéger l'industrie de défense.

Le directeur de la DSEZP

PROTECTION

Contrats défense, quelles obligations/contrôles pour les sous-contractants?

Tout sous-contractant d'un contrat avec détention d'informations ou de supports classifiés (ISC) ou avec accès à des ISC doit être **habilité**. En cas de contrat avec détention d'ISC, le sous-contractant doit en outre assurer la **sécurisation physique de ses locaux et systèmes d'information**. Une **annexe de sécurité spécifique** au sous-contrat sera nécessairement établie, distincte de l'annexe de sécurité du contrat principal. Y seront mentionnées les missions du sous-contractant, les dates de travaux d'exécution ainsi que les ISC auxquels il aura accès.

Des **visites et inspections** de la Direction du Renseignement et de la Sécurité de la Défense (DRSD) ou de l'autorité contractante permettent de contrôler le respect et la bonne application de ces mesures de sécurité. Des **actions correctives** peuvent être exigées si nécessaire.

En matière de recours à des **sous-contractants étrangers**, le Secrétariat général de la défense et de la sécurité nationale (**SGDSN**) est compétent pour vérifier l'équivalence du degré de protection des ISC entre les parties contractantes. Il peut à cette fin **négocier des accords de sécurité** avec **l'autorité d'habilitation nationale** afin qu'elle procède à une habilitation appropriée de l'entreprise étrangère.

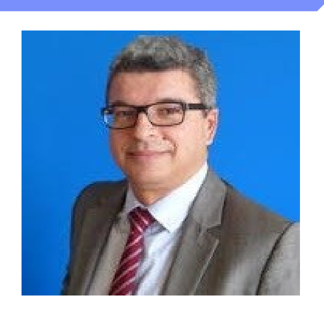
Il convient de se **rappeler** que le **sous-contrat** entre une entreprise française et une entreprise étrangère **n'est pas envisageable** lorsqu'il **prévoit** la détention ou l'échange **d'ISC** portant la **mention *« Spécial France »*.**

Cas pratique: une société de droit français X souhaite sous-traiter une partie de l'exécution de son programme d'armement à une société asiatique. Il s'avère que cette entreprise n'a pas les mêmes standards en matière d'habilitation de son personnel et qu'il y a absence d'accord de sécurité bilatéral entre la France et l'Etat de nationalité de l'entreprise. Le SGDSN considère que malgré une éventuelle habilitation de l'entreprise asiatique par l'autorité nationale compétente, la sous-traitance présenterait des dangers pour la protection des ISC français. Des négociations peuvent alors être mises en place par le SGDSN et l'autorité d'habilitation étrangère afin d'établir une réglementation propice à une protection équivalente des ISC.

Instruction Générale Interministérielle n°1300 sur la Protection du secret de la défense nationale, Article 97 « Cas des entreprises étrangères ».

ENTRETIEN

Avec M Zoheir BOUAOUICHE, sous préfet d'Etampes et chargé de mission IET en Essonne



DSEZP : Monsieur le sous-préfet, pouvez vous préciser quelles sont vos attributions dans le cadre de **l'IET** ? Et aussi comment le département est il impliqué, dans une politique de l'IE qui concerne de nombreux acteurs ?

M. BOUAOUICHE : l'intelligence économique territoriale est **l'intelligence économique** adaptée aux particularismes propres à chaque **territoire**. L'organisation actuelle de l'État en cette matière repose sur un pilotage de cette politique publique assuré par le Préfet de Région, en charge de la rédaction d'un schéma régional de l'intelligence économique, de la réunion d'un comité régional *ad hoc* et de la définition des priorités d'action dans une feuille de route annuelle déclinée ensuite par les Préfets de départements.

En tant que **référent IE**, désigné par la Préfète de l'Essonne, j'ai donc en charge **l'animation** et **l'accompagnement** de cette politique publique dans le **département**, c'est-à-dire :

- **faciliter le dialogue** en la matière entre services de l'Etat, structures publiques, académiques, collectivités territoriales et organismes privés ;
- **faire le lien** entre le **niveau national**, l'échelon **régional** et le **local** ;
- **être l'interlocuteur privilégié des entreprises** et acteurs du territoire en **matière d'IE**.

DSEZP : Quelles sont, d'après votre expérience, les menaces les plus prégnantes pouvant concerner les sociétés dans votre département ?

M. BOUAOUICHE : Souvent, l'intelligence économique est associée à la notion de menace et réduite à son volet « sécurisation ». Il faut rappeler **qu'il s'agit avant tout** d'une démarche qui contribue à identifier des **opportunités économiques**. L'intelligence économique à travers ses missions de **veille**, **d'influence** et de **sécurisation** s'inscrit dans la perspective du **renforcement de la compétitivité** et du **soutien au développement économique**. Défis majeurs des pouvoirs publics.
Néanmoins, pour répondre à votre question, j'évoquerai les **rançongiciels** qui menacent les données et les finances des entreprises, les **escroqueries financières**, qui exploitent les failles organisationnelles des entreprises et toutes les menaces qui pèsent sur le **patrimoine immatériel des entreprises** et plus particulièrement celui lié à **l'innovation ou la R&D**.

DSEZP : Comment pouvez-vous, concrètement, apporter une aide aux entreprises ?

M. BOUAOUICHE : Au-delà de la simple écoute, mon **rôle** est de **réunir les bons interlocuteurs** en matière d'IE autour des projets des entreprises ou de leurs interrogations, qu'il s'agisse de services de l'État, de partenaires publics (Collectivités, Consulaires…), académiques ou économiques. Cet **accompagnement** concerne **toutes les entreprises** et tous les laboratoires de recherche, quel qu'en soit leurs statuts ou leurs tailles. Par ailleurs, mon **action** vise également à favoriser la réalisation de démarches de **sensibilisation** ou de **formation** à destination de ces mêmes publics, en association avec tous les partenaires et experts de la question.

DSEZP : Merci, Monsieur, pour ces réponses qui permettent de mieux cerner les enjeux de l'IET.

Infos utiles:

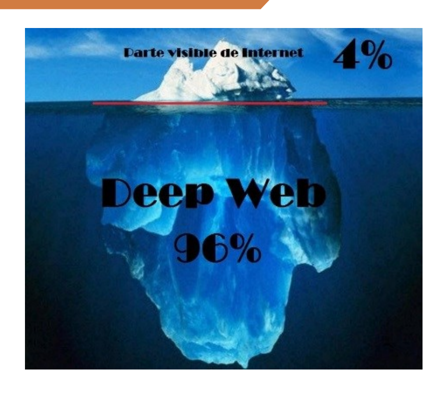
39 000 entreprises en Essonne

Filières d'excellence :
- **Biotechnologies**
- **Optique**
- **Eco-technologies**

Contact
Sous-préfecture d'Etampes
01 69 91 91 91

CYBER

LE WEB



Le *Web* tel que nous le connaissons généralement désigne la partie de la toile accessible en ligne et indexé par les moteurs de recherche courants : *Google*, *Yahoo*, *Yandex* (Russie), *Baidu* (Chine), etc.
Il est admis que ce *web* surfacique représente environ **4%** des données.
Les **96%** restant communément appelés ***web* profond** ou ***deepweb***, désignent la toile accessible en ligne, mais non-indexée par les moteurs de recherche classiques.
Finalement, c'est bien à la structure de sécurité de connaitre ce monde et, en connaissance de cause, mener une **politique** de **sécurité adaptée** à cet espace stratégique.

Les différents niveaux du *Web*



Niveau 1 : le *web* commun
Ce niveau est celui sur lequel vous naviguez tous les jours : *YouTube*, *Facebook*, *Google*, *Wikipédia* et d'autres sites célèbres ou facilement accessibles donc indexés.



Niveau 2 : le *web* de surface
Ce niveau est accessible par des explorateurs habituels, mais contient des sites internet « sombres », tels que *Reddit*, les services d'adresses e-mail temporaires, les téléchargements illégaux en direct, les hébergements de web, les bases de données MYSQL etc.



Niveau 3 : le *web* des téléchargements
Vous pouvez y trouver des sites « *underground* » mais toujours indexés, comme *4chan*, *Freehive*, *Hell bound*, les téléchargements illégaux par *Torrent*, des résultats de recherche *Google* bloqués.

À partir du niveau suivant, l'utilisation d'un *Virtual Privat Network (VPN)* et du réseau TOR est obligatoire et de solides connaissances en informatique sont requises.



Niveau 4 : le *Web* profond ou *Deep Web* (instructif)
S'y cachent des forums en tout genre et de tout type : drogue, films ou livres interdits, codes sources de virus, discussions entre hackers.



Niveau 5 : le *Web* profond (activiste)
Ce *Web* est strictement anonyme et particulièrement difficile à tracer (mais pas impossible). Ici, beaucoup de sites fonctionnent sur le réseau *Onion* : sites de ventes de drogues, d'armements, d'êtres humains, des sites pédopornographiques, des groupes de pirates (*anonymous*, *lizard squad*, *syrianelectronicarmy*, etc.) et pour finir des groupes terroristes comme *Daesh*.

Ce qu'il faut retenir :
Dès le niveau 2 vous pouvez être dans l'illégalité.
Un simple accès au niveau 5 vous expose à des poursuites judiciaires car le *Web* profond est devenu l'une des priorités des gouvernements.



Dans le cadre de votre entreprise :
- **Surveillez** vos passerelles vers Internet par la mise en place d'outils de journalisation des activités sur le *Web*.
- Si possible, **mettez en place des listes de sites interdits** ou forcez les navigations sur une liste des sites autorisés.
- **Privilégiez la saisie manuelle des sites** que vous souhaitez visiter ; ne cliquez pas sur des liens proposés par d'autres sites *Web*.

Pour toute question supplémentaire veuillez contacter :
dpsd-dsezp-ssi.cds.fct@intradef.gouv.fr



INTELLIGENCE ECONOMIQUE

Le fait religieux dans l'entreprise

Le fait religieux dans l'entreprise mobilise actuellement l'ensemble des acteurs du monde économique. Souvent source d'inquiétudes mais aussi de questionnement, le sujet doit être maîtrisé à la fois par la chaîne sûreté et par le management, qui, en symbiose, auront à fixer les règles et à y faire adhérer les collaborateurs. Lesquelles règles auront à être respectueuses de la liberté individuelle et soucieuses de la mission de l'entreprise.

Ainsi, le 28 novembre le colloque du MEDEF IDF a-t-il traité ce thème sous la forme de trois tables rondes où se sont exprimés : des entrepreneurs, des responsables sûreté, des institutionnels et un avocat. Après une introduction faite par le SCRT sur le phénomène de radicalisation, Me Thibault du Manoir de Juaye a donné un aperçu des derniers cas traités par la justice et de l'état de la jurisprudence.
Soulignons que, l'entreprise a deux leviers principaux pour agir sur la question :

- Un règlement intérieur (jurisprudence PAPREC).

- Le contrat de travail.

Annoncé par Mme EL KHOMRI le 07 novembre, un « guide du fait religieux dans l'entreprise » doit être publié sous peu. Déjà disponible sous forme de document de travail, ce questionnaire traite, à travers 39 questions/réponses appuyées par une jurisprudence, les thèmes les plus souvent évoqués dans ce domaine.

Pour aller plus loin:
Publication très prochainement du guide « fait religieux dans l'entreprise » sur le site : travail-emploi.gouv.fr

Après la DPSD, pourquoi la DRSD ?

Le nouveau nom de la DRSD est effectif depuis le 07/10. Ses missions historiques perdurent : la sécurité du personnel, des installations et des systèmes d'informations du ministère reste au cœur des préoccupations du Service. Mais, **le volet « renseignement »** prend une nouvelle dimension et devient **prépondérant**.
Par ailleurs, l'essor du **« cyber »** constitue l'un des éléments de cette **transformation**.
Principaux objectifs :
La **lutte antiterroriste** et la **protection du potentiel scientifique et technique de la nation (PSTN)** sont les 2 principaux objectifs opérationnels qui mobilisent aujourd'hui le Service.

SOPHIA : le contrôle qualité de l'OS

Si le renseignement de la fiche 94A est bien du ressort de l'intéressé, c'est à l'OS qu'il revient de contrôler les informations saisies. **Cette vérification est en quelque sorte le « contrôle qualité » qui permettra d'éviter qu'une procédure soit rejetée.** Le système SOPHIA refuse en effet toute fiche incomplète ou incorrectement renseignée.

Externaliser ses données ?

Suite à une proposition commerciale faite à un client, une société se voit ravir le marché par un concurrent. L'incident se reproduit à plusieurs reprises. Après enquête de l'équipe cyber de la DSEZP, il s'avère que le système informatique et notamment les prospects commerciaux étaient externalisés chez un hébergeur privé et de plus piraté.
En conclusion, il est impératif pour l'entreprise de se poser les questions :

- comment gérer mes données ?
- qui doit y avoir accès ?
- les données constituant mon patrimoine immatériel peuvent-elles être externalisées ?

Ainsi, et à l'instar d'autres risques, c'est en toute connaissance de cause que vous assurerez la protection de votre patrimoine.

Pour toute question complémentaire veuillez contacter :
dpsd-dsezp-ssi.cds.fct@intradef.gouv.fr